



CVE-2021-32632

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-32632
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-20 16:15:00 UTC
Updated	2021-05-27 01:31:00 UTC
Description	Pajbot is a Twitch chat bot. Pajbot versions prior to 1.52 are vulnerable to cross-site request forgery (CSRF). Hosters of the

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pajbot	Pajbot	All	All	All	All

References

Reference	Source	Li
Release v1.52 · pajbot/pajbot · GitHub	MISC	gi
Pajbot CSRF Vulnerability Test · GitHub	MISC	gi
CSRF allowing modification of commands, modules, banphrases through hidden iFrames · Advisory · pajbot/pajbot · GitHub	CONFIRM	gi
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report